


REPORT		AD-A238 474		REPRODUCTION PURPOSES	
Public report to be distributed to the public in accordance with the provisions of the Data Rights Act of 1980 (50 USC 1501-1504) and the Department of Defense Policy on the Release of Information (DoD 5400.7-R).				Form Approved OMB No. 0704-0188	
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE April 91		3. REPORT TYPE AND DATES COVERED Final 22 Oct 90 - 21 Apr 91	
4. TITLE AND SUBTITLE Multi-level Security System for Amphibious Operation Command and Control				5. FUNDING NUMBERS DAAL03-91-C-0007	
6. AUTHOR(S) Eldon R. Landers, John E. Price, Dave Alexander					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Savannah River Associates, Inc. 201 South Main Street Dumfries, Virginia 22026				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING MONITORING AGENCY NAME(S) AND ADDRESS(ES) U. S. Army Research Office P. O. Box 12211 Research Triangle Park, NC 27709-2211				10. SPONSORING MONITORING AGENCY REPORT NUMBER ARO 28522.1-EL-SBI	
11. SUPPLEMENTARY NOTES The view, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.					
12a. DISTRIBUTION AVAILABILITY STATEMENT Approved for public release; distribution unlimited.				12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) This report documents the performance of Savannah River Associates, Inc. on the "USMC Multi-level Security System for Amphibious Command and Control" contracts and cites the results of studies and surveys conducted to meet requirements of the program. The document further analyzes the alternatives available to the Marine Corps for achieving the desired system capability and in the attached document, "MLSS Paper Prototype", provides a recommended course of action for a successful Phase II SBIR effort which can reasonably be expected to transition to a Phase III SBIR program.					
14. SUBJECT TERMS				15. NUMBER OF PAGES 13	
				16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED		18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED		19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	
				20. LIMITATION OF ABSTRACT UL	

91-05286



1.0 Introduction.

The Marine Tactical Command and Control System (MTACCS) is an "umbrella" concept which envisions an integrated, automated command and control system with organic communications which can support the tactical operations of the Marine Air Ground Task Force (MAGTF) at all echelons of command. An integrated Command, Control, Computers, Communications, Intelligence and Interoperability (C⁴I²) systems approach is the mainstay of the Marine Corps Field Demonstrations System for command and control (C²) development. Field demonstrations provide an evolutionary development test bed for a number of MAGTF functional elements using equipment and systems that are already in the inventory as well as non-developmental and commercial-off-the-shelf items. Specifically, these elements include:

- Command, Control, Computers, Communications, Intelligence and Interoperability (C⁴I²) Systems for:
 - Ground C²
 - Aviation C²
 - Combat Service Support (CSS) C²
- Approved C² architectures that synthesize the placement and use of tactical C⁴I² systems
- Supporting communications equipment
- C³I systems on board amphibious ships
- Common hardware and software
- Interoperability requirements and standards programs
- Configuration management.

The Multi-level Security System (MLSS) project is an essential element of the Combat Information Processor (CIP) Advanced Technology Transition Demonstration (ATTD) which serves to demonstrate advanced concepts in Amphibious Operations Command and Control (AOC²) software and hardware, suitable for further development and integration into USMC command and control systems. The requirements which drive the MLSS project emanate from the operational specifications of the MTACCS concept (Figure 1-1). The open architecture concept of the CIP and the MLSS efforts provides the flexibility necessary for the MLSS to be applicable to a variety of potential AOC² concepts.

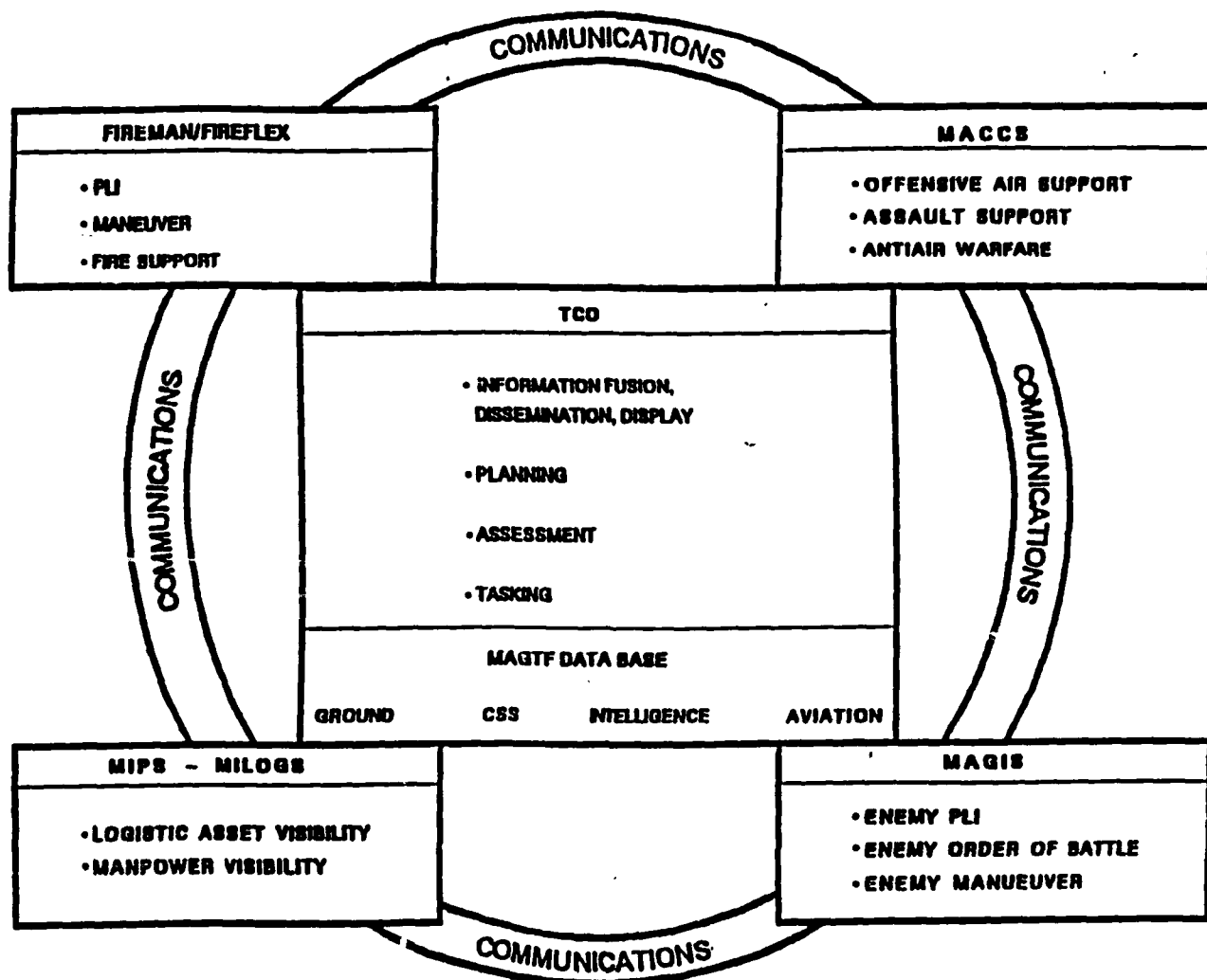


Figure 1-1 Marine Tactical Command and Control System (MTACCS)

1.1 Project Initiation.

The "Multi-level Security System (MLSS) for Amphibious Operation Command and Control" Small Business Innovative Research (SBIR) proposal was selected for contract award April 13, 1990 and the contract was effective as of October 22, 1990, with modification on November 06, 1990.

1.2 USMC MLSS Project.

Over the six month period the MLSS Phase I effort entailed the examination of the CIP ATTD hardware, software, and associated documentation, in order to:

- Define the security requirements for the Marine Corps AOC²

- Perform a survey of the commercial market place for non-developmental items (NDI) and commercial-off-the-shelf (COTS) products that could provide possible solutions to the MLSS requirements
- Evaluate the alternatives open to the Marine Corps that would lead to the successful application of the MLSS
- Identify potential Phase III markets for the MLSS
- Identify potential support from the commercial sector for Phase II and Phase III efforts
- Obtain a commitment from the commercial sector for a Phase III effort.

2.0 Security Requirements.

The AOC² envisions the highest classification of information stored in the system to be SECRET. Users of the system would be Marines with access authorizations ranging from UNCLASSIFIED through SECRET. DoD Directive 5200.28, Security Requirements for Automated Information Systems, is the governing regulation for defining the security features which a system must meet to achieve various levels of secure operations. This regulation defines the security classification levels ranging from C1 at the lowest through C2, B1, B2, and B3 to A1 at the highest level. Twenty-seven aspects of security are defined for specifying security features. The level of security attained by the implementation of these security measures is defined for each of the security classes.

The directive also defines procedures for determining the appropriate security class a specific system must achieve. A system which contains up to SECRET information to be accessed by individuals with access authorization varying from UNCLASSIFIED to SECRET is defined as a multi-level system and will require a security classification of B2. This directive forms the basis for the accreditation authority's determination to accredit a specific system.

When a new system which processes classified information is to be built, the most timely and efficient way to achieve the necessary security features is to build upon an operating system which affords the required security class. The application then only has to make use of the existing features and do nothing to violate the operating system's base security features.

3.0 Commercial Survey.

A search of commercially available products revealed no available workstation operating system evaluated at the B2 security class upon which to develop the CIP application. The survey further revealed that a commercially available B2 workstation operating system

may not be available for some time. As a consequence, it will be necessary to start with a system evaluated at a lower security class level and to add the additional features required to achieve multi-level security accreditation.

Two products are currently available and certified at the lower security class of B1. The AT&T UNIX System V/MLS has been certified, but it is available only on a limited number of platforms which do not include the CIP hardware configuration. The other available B1 product is the Compartmented Mode Workstation (CMW) developed by SecureWare on the Apple UNIX operating system.

When comparing these two platforms, CMW affords the best alternative for developing this application. The standards for the CMW are defined by the Defense Intelligence Agency in DDS-2600-5502-87, Security Requirements for System High and Compartmented Mode Workstations. The CMW standard is an extension of DoD Directive 5200.28. It requires all of the features of a B1 security class, but includes components defined for the B2 and B3 levels. An additional feature of the CMW not discussed in the DoD Directive is the definition of a user interface built on X-Windows. This interface relieves the system developer of the need to develop these features. The availability of this user interface and the additional B2 and B3 features makes the CMW a far better platform on which to build the additional features required for multi-level security accreditation.

Four additional CMWs will be available in the future. They are based on the Intel 386, IBM, Sun and Digital hardware platforms and are being developed by four additional vendors. In addition to the Apple, SecureWare has either completed a port or is in the process of porting it's system to fifteen different platforms. Of these, none have been evaluated by the National Computer Security Center (NCSC), at this time. Discussions with SecureWare indicate that porting their CMW system to the CIP hardware configuration should pose no problems.

When it is necessary to add security features in addition to those provided by the operating system, add-on products are often available. This is particularly true for the IBM mainframe environment. An additional commercial product search was conducted to determine if add-on security products were available which could be added to the current CIP platform and operating system. The search revealed no NCSC evaluated add-on security products.

4.0 Alternatives.

Based on the results of our studies in Phase I, two feasible approaches for achieving multi-level security operations for the CIP application exist. The first approach is to add security features to the current CIP operating system and application. The second approach would call for migrating the CIP application to a B1 CMW and then adding the security features needed to achieve multi-level security accreditation. The following

sections describe each approach and our assessment of it.

4.1 First Approach, CIP Application Software Enhancement.

The first approach for achieving multi-level security for the CIP application is to identify the requirements for achieving multi-level security accreditation and then add software enhancements to meet these requirements. This approach entails working with Marine Corps Research, Development and Acquisition Command (MCRDAC) and Harry Diamond Laboratories (HDL) to determine the accreditation authority for the CIP and to the initiation of discussions with that authority to secure guidance and direction in the security enhancement effort. The CIP operating system and application software would then be analyzed to determine what modifications and additions would be needed to meet the accreditation requirements. Finally, the necessary changes would be incrementally added to the CIP and the entire system would be regression tested.

Multi-level security was not a consideration for the developers of the CIP. As a result, this approach would require a great deal of time and money. The lack of multi-level security consideration during the operating system and application design could prove to be a problem during accreditation. A large amount of new documentation would be required by the accreditation authority.

4.2 Second Approach, CMW.

The second approach for achieving multi-level security for the CIP application is to migrate the CIP application to a B1 CMW and then to add security features needed to achieve multi-level security accreditation. This approach requires identifying the accreditation authority for a MLSS and begin discussing accrediting the CIP application on the CMW. The discussions would secure guidance and direction for the migration effort. The CIP application software would be analyzed to identify the enhancements required to achieve a multi-level security accreditation. At the same time, the issue of porting the application to the CMW environment would be addressed. Once all the requirements are known and the enhancements have been identified, the probability of successful accreditation can be determined and an estimate to complete can be made. An implementation schedule would then be prepared and the CIP application would be ported to the B1 environment. Any security enhancements would be added and tested at this point.

Savannah River Associates performed an in-depth study to determine the most appropriate platform for this approach. A survey of the existing workstation base in the Marine Corps and the DoD identified the Intel 386-based workstation as the most widely deployed hardware platform. A look at future workstation procurement indicates that these workstations will continue to be the mainstay of the Marine Corps. Adding to that the immediate availability of a Beta-test version of SecureWare's CMW for the Intel 386-based workstation, SHA feels that the Intel 386-based workstation is the most appropriate

hardware platform for the CIP application migration. No other hardware platform appears to have the advantages of the Intel 386-based workstation. Although the CIP development system is a Sun Microsystems workstation, no CMW operating system will be available before Spring 1992. The SecureWare CMW is the most appropriate operating system because of its B1 accreditation on the Apple Macintosh and the near term availability of their Intel 386-based workstation CMW. Additionally, SecureWare had demonstrated to SRA a willingness to provide extensive support to the CMW porting effort, and more importantly, a commitment to a Phase III effort. We feel that this approach has the greatest probability of satisfying the MLSS objectives and producing a fieldable C² system for the Marine Corps within budgetary and time constraints.

5.0 Phase III MLSS Applications.

Successful completion of Phase II will produce a multi-level security prototype and an extensive knowledge-base about porting existing software into the CMW environment. The MLSS prototype will be a multi-user, multi-function, open architecture C² system based on the CIP. As a result of the developmental flexibility afforded by the open architecture concept, the MLSS prototype has potential applications throughout the DoD community, other Federal agencies, and the commercial arena. Based upon information obtained from discussions held during Phase I investigations, we have identified a number of users for the MLSS prototype and for the lessons learned during its development. The following sections outline who can benefit in Phase III from the Phase II project and how.

5.1 Defense Intelligence Agency.

DIA initiated the development of CMW's as early as 1985. It awarded five development contracts in 1988, of which SecureWare is the first and only firm to have completed its accreditation. The MLSS will serve as a proof-of-concept for the CMW. By establishing multi-level secure communications between multiple CMW's using the MACSIX protocol, the MLSS prototype goes far beyond anything DIA has currently developed. It would be a valuable aid in shaping the future of the CMW in the national intelligence community. The lessons learned during the CIP software port can be used by DIA project managers to better guide the incorporation of applications into the CMW. The prototype can also serve as a development test bed, providing DIA with a valuable platform on which to study the effects of introducing the CMW to its analysts.

5.2 U.S. Navy.

The close operational relationship that exists between the Navy and the Marine Corps makes the Navy a natural candidate for application of the MLSS. The MLSS will provide the Navy with a multi-level security environment into which they can easily migrate existing applications. The ability to port applications into the CMW environment will reduce the need for costly redevelopment efforts. The CMW environment will provide Navy developers with an excellent environment for application programming. The MLSS can

be ported to virtually any hardware suite supporting UNIX. The CMW's design ensures a relatively simple and inexpensive porting effort. Installing the MLSS on existing hardware will be easy and provide an enormous savings; in terms of both time and money. Its open architecture, distribution of functionality, and the portability of CMW ensure easy expansion and proliferation of the MLSS. Using the MLSS as a base would provide the Navy with interoperability on a scale not possible at present. The MLSS would provide the Navy with an inexpensive way to leap into the 21st century today.

5.3 DoD and Other Agencies.

The MLSS prototype will be a very flexible and very portable platform into which numerous applications can be introduced. Its use of the MACSIX protocol for inter-processor communications enables it to support a high degree of interoperability for any application and for any user group. These features ensure that the results of Phase II would be marketable to more than one service, more than one agency, and be appropriate to a variety of commercial applications.

5.4 Phase III Summary.

As a result of SRA's survey of the commercial market and coordination conducted with elements of DIA, SecureWare, Inc. of Atlanta, Georgia appears to be the leader in the CMW field. Since our study indicated that the most likely approach to succeed in the development of the MLSS involved the CMW application, SecureWare was approached and a working association was developed. SecureWare has clearly demonstrated the vision and willingness to assist SRA's Phase II effort, and subsequently, to commit to a Phase III effort projected at the DoD community, other Federal agencies, and specified commercial firms. An SRA/SecureWare association presents a most effective and potentially successful MLSS Phase III program.

Attachment 1. Paper Prototype

1.0 Description of Prototyping Effort.

Savannah River Associates proposes to implement the approach described in paragraph 4.2 of the Final Report to achieve a prototype Multi-Level Security System (MLSS). Expanding on the description of this approach, the following describes in detail the prototyping effort.

1.1 Prototyping Environment.

We propose to migrate the CIP application from its current hardware suite to an Intel 386-based suite utilizing Compartmented Mode Workstation operating system from SecureWare, Inc. The prototype hardware suite will contain a message handling processor, a database processor, and a user interface processor, Figure 1. Each Intel 386 processor will include an 80387 math co-processor and at least 64K bytes of cache memory for performance enhancement.

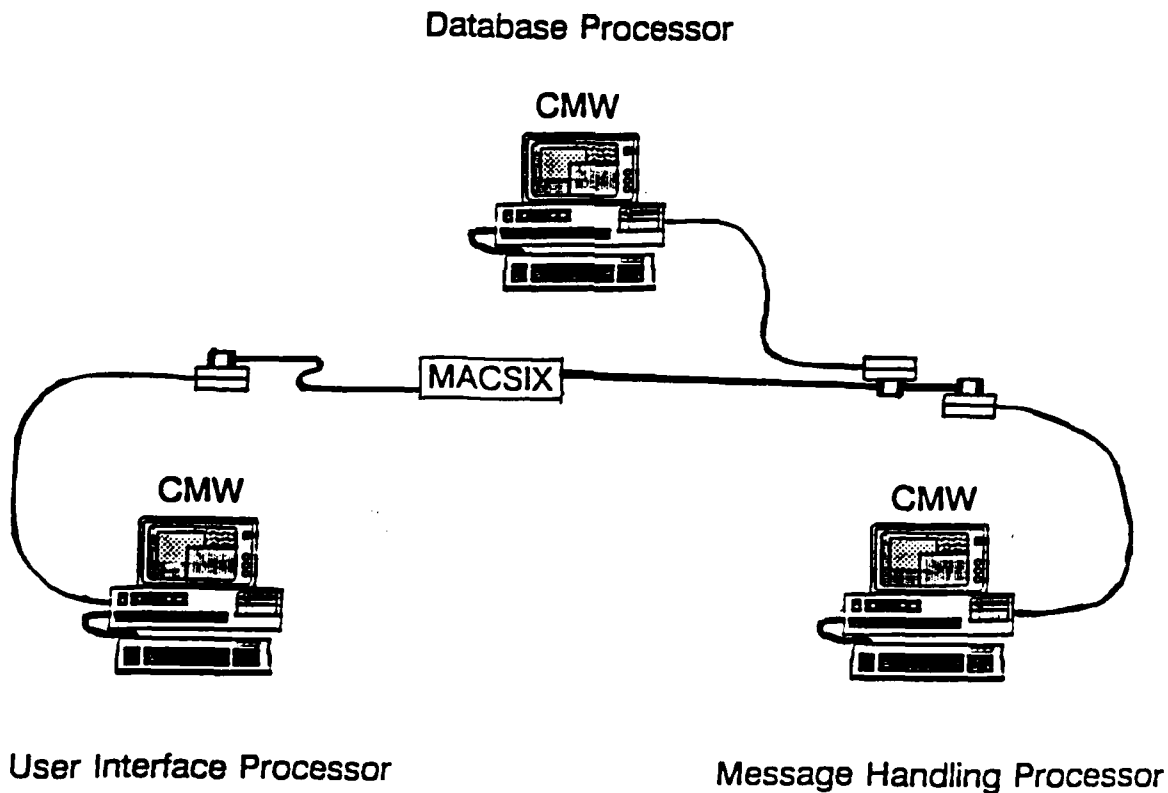


Figure 1. MLSS Prototype Configuration

The processors will communicate with each other across a local area network. CMW's must pass both sensitivity and information levels for the data they pass when they communicate. DNSIX is the DoDIIS protocol for network communications. DNSIX, however, does not accommodate the passing of information levels. Therefore, the MACSIX protocol provided by SecureWare's CMW will be used. The SecureWare, Inc developed MACSIX is an extension of the DNSIX protocol.

SecureWare's CMW product has been ported from the Apple Macintosh to the Intel 386 hardware and is currently available as a Beta-test version. This version is functionally equivalent to the B1 evaluated Macintosh version. SecureWare is awaiting evaluation of the Intel 386 version by DIA and the NCSC. The prototype configuration provides a test bed with which to evaluate the MLSS as a multi-user, multi-function, open architecture.

1.2 Prototyping Activities.

The prototyping effort is broken into two sub-phases. The first sub-phase focuses on identifying the procedures involved for receiving accreditation of the MLSS, on familiarizing ourselves with the CIP application, on identifying the additions and modifications needed to meet the accreditation requirements, and on determining the effort required to port the CIP application software to the CMW environment. The second sub-phase will accomplish the software port and implement the security enhancements required for accreditation. Each sub-phase is described in greater detail in the following sections.

1.2.1 Sub-phase One.

Sub-phase One begins with the identification of the accreditation authority for the MLSS. The accreditation authority will play a major role in determining the effort required to achieve the MLSS. We will work closely with the accreditation authority to determine the exact procedures to be followed and the requirements to be met in order for the MLSS to be accredited. Because each processor in the configuration is assigned a separate, unique task, the entire local area network must be accredited as the complete MLSS. This will complicate the accreditation process making close contact with the accreditation authority an absolute must. At the same time, we will work in coordination with Harry Diamond Laboratories to secure a copy of the CIP software and documentation in order to become familiar with the application software. The SUN-based development system will be sufficient for this purpose.

During our familiarization with the application software, we will identify the modifications and additions which will be required to provide the security enhancements needed to meet the accreditation requirements. We will maintain a close relationship with the accreditation authority to ensure that our designs will meet their requirements. SRA will also maintain its close relationship with PRC, Inc., who have committed to providing their expertise in software analysis, porting and design. Savannah River Associates will also

establish a close relationship with SecureWare, Inc during the analysis of the CIP software. This relationship will allow us access to the CMW security model and will enable us to identify conflicts between the CIP software and the CMW. When conflicts are found, we will be able to use SecureWare's expertise to identify the most appropriate software change. We envision that all changes will be done to the application software. We do not intend to modify the CMW trusted computer base.

We will produce a technical report at the conclusion of our CIP software analysis. This report will document the accreditation procedures and requirements, the detailed design of any proposed security enhancements, and the detailed design for any modifications identified for a successful software port. The report will present Savannah River Associates' opinion on the probability of successful accreditation, and an estimate to complete for the MLSS. This report will be delivered approximately six months after the initiation of Phase Two. Six months is a reasonable amount of time for Sub-phase One considering the lack of reported documentation for the CIP software.

1.2.2 Sub-phase Two.

The second sub-phase will accomplish the actual porting of the CIP software to the Intel 386-based hardware suite. The initial effort during this sub-phase will be to install the CMW package on each processor and establish communications between the processors over the local area network. This activity will follow the guidelines provided by the accreditation authority. We envision this set up taking place before the end of the first sub-phase. This will allow us to familiarize ourselves with CMW and its security model and will allow us to test design feasibilities during Sub-phase One. After the review and discussion of the first sub-phase technical report, we will begin the process of porting the CIP software to the prototype hardware suite. The methodology to be followed during the port will be determined using the results of the first sub-phase. At this time, we anticipate the following scenario:

- Implement software on each processor as a stand-alone application
- Add initial security enhancements to each processor's application
- Establish communications between the database processor and the user interface processor and between the database processor and the message handling processor
- Add final security enhancements to the prototype
- Verify and validate the prototype system.

The actual methodology followed will be based on the results of the detailed analysis performed during the first sub-phase and on the procedures and instructions given by the

accreditation authority. During Sub-phase Two, we will continue a close relationship with the accreditation authority to ensure a smooth accreditation process. It is important that we know exactly what is expected by the accreditors and that they know exactly what we have done. It will also be important for us to maintain our close relationships with PRC, Inc. and SecureWare, Inc. Their combined expertise will allow us to resolve any application/CMW conflicts quickly and easily. They will also provide us with the knowledge needed to fine tune the CMW's performance within the prototype environment. The actual work to be completed in Sub-phase Two will be determined during the review and discussion of the Sub-phase One technical report. It may develop that the accreditation authority wishes an accreditation plan written. The preparation of this plan or other documentation which may be desired is not included in our assessment of Phase Two work and will be subject to later negotiation.

Annex A Summary of Prototyping Activities

This annex provides a summary of the expected activities involved in the production of the MLSS. The activities described for Sub-phase II are subject to change upon completion of Sub-phase I.

Sub-phase I

- Locate accreditation authority and begin discussions on MLSS accreditation
- Set up Sun workstation laboratory and install CIP application software
- Begin familiarization with CIP application software and review existing documentation
- Identify modifications and additions required to provide security enhancements needed to meet the accreditation requirements
- Continue discussions with accreditation authority, seeking general approval of enhancement designs
- Working in coordination with SecureWare, locate any security policy conflicts between CMW and the CIP software
- Produce technical report documenting the accreditation procedures and requirements, the detailed design of any security enhancements, and the detailed design of any modifications needed for successful software porting.
- Conduct technical review to establish work plan for Sub-phase II and to finalize MLSS objectives.

Sub-phase II

- Set up prototype hardware and install CMW package on each processor
- Establish communications between each processor across the local area network
- Begin familiarization with CMW package and its security policies
- Port CIP application software to the appropriate processor and establish stand-alone operations
- Add security enhancements to each processor's application

- Continue seeking guidance and direction from the accreditation authority
- Establish communications between the database processor and the user interface processor and between the database processor and the message handling processor using the MACSIX protocol
- Add final security enhancements to the MLSS prototype
- Under the guidance of the accreditation authority, verify and validate the prototype system
- Complete any additional tasks required by the accreditation authority, as appropriate.